Programmable CBDCs, Digital Identity, ISO 20022, and AI: Reconfiguring Power in Payment Infrastructures

Sixbert Sangwa*[1], Placide Mutabazi[2]

[1]Department of International Business and Trade, African Leadership University, Kigali, Rwanda

[2]Office of the Executive Chancellor, Open Christian University, California, the United States

*Corresponding Author: ssangwa@alueducation.com

CITATION

Sangwa S. and Mutabazi P. (2025). Programmable CBDCs, Digital Identity, ISO 20022, and AI: Reconfiguring Power in Payment Infrastructures. Open Journal of Stewardship Economics & Ethical Innovation. Vol 01. Issue 02. Open Christian Press.

DOI:
https://doi.org/10.5281/zenodo.17179094

ARTICLE INFO

Received: 20 September 2025
Published: 22 September 2025
Category: Original Article

COPYRIGHT

Copyright © 2025 by author(s).

***Open Journal of Stewardship Economics & Ethical Innovation* is published by Open Christian Press. This work is licensed under the Creative Commons Attribution (CC BY) license.**
https://creativecommons.org/licenses/by/4.0

PUBLISHER INFO

Open Christian Press—the publishing arm of Open Christian University—is produced in partnership with the Center for Faith and Work.

***Disclaimer:** The views expressed are solely those of the authors and do not necessarily reflect their institutions.*

Abstract: ***Purpose:*** This study interrogates the convergence of programmable central-bank digital currencies (CBDCs), national digital-identity regimes, ISO 20022 data standards, and AI-driven regtech to determine how their fusion redistributes gatekeeping authority within modern payment infrastructures. ***Design/methodology:*** Through comparative content analysis of policy papers, pilot reports, and regulatory texts from the European Union, United Kingdom, China, Nigeria, and cross-border projects such as BIS mBridge, the article couples empirical evidence with three theoretical lenses—weaponised interdependence, Foucault's governmentality, and Mann's infrastructural power. ***Findings:*** Results reveal that these intertwined technologies promise efficiency and inclusion yet simultaneously centralise control in the "rails" of the financial system, enabling transaction-level programmability and finely grained sanctions. Liberal jurisdictions seek to diffuse power through privacy thresholds and shared governance, whereas more authoritarian models exploit identity binding and real-time surveillance to extend state reach. Limited adoption in Nigeria illustrates that technical capability alone cannot confer infrastructural authority without public trust. ***Originality/value:*** Integrating economic sociology with Christian ethical analysis, the article devises a normative test drawn from scriptural principles—honest scales (Prov 11:1), Jubilee resets (Lev 25), and freedom of conscience (Rev 13:17)—to evaluate whether emerging architectures entrench coercive leverage or foster economic justice. ***Practical implications:*** Policymakers should codify privacy by design, guarantee offline or bearer-style options for small payments, legislate transparent limits on programmability, and promote multipolar governance to avert new monopolies over *"who may buy and sell."* ***Social implications:*** Embedding mercy, accountability, and pluralism at the protocol layer is essential if digital money is to enhance, rather than erode, human dignity and freedom.

Keywords: central bank digital currency; digital identity; ISO 20022; programmable money; AI in payments; financial gatekeeping; infrastructural power

1. Introduction

Across many jurisdictions, payments are rapidly moving toward an identity-bound, data-rich, and programmable paradigm. Central banks worldwide are deeply engaged in CBDC development: 91% of 93 surveyed central banks in 2024 reported exploring retail and/or wholesale CBDCs, with wholesale interbank pilots generally more advanced than retail projects (Illes et al., 2025). Several smaller economies have even launched retail CBDCs (e.g. in the Bahamas, Jamaica, and Nigeria), albeit with limited adoption to date (Unlock Blockchain, 2025). This push for digital fiat currency is situated within a broader shift toward *tokenization* of assets and programmable settlement features, especially on the wholesale side of finance (Unlock Blockchain, 2025).

In parallel, governments are standardizing digital identity frameworks to anchor this new financial infrastructure. Notably, the European Union (EU) in 2024 adopted Regulation (EU) 2024/1183 establishing a bloc-wide *European Digital Identity* (EID) and wallet recognized across member states (EU, 2024). This regulation mandates that by 2026 every EU citizen and business shall have access to a secure digital identity wallet enabling cross-border authentication and credential sharing (EU, 2024).. The EID wallet links national IDs to a user-controlled data wallet for verifying attributes (e.g. licenses, bank accounts) with privacy safeguards (e.g. selective disclosure, pseudonyms) (EU, 2024).. Similar digital ID initiatives are underway elsewhere, from India's Aadhaar-linked payment apps to Nigeria's eNaira which requires identity verification via banks. These trends point to convergence of money and identity: transactions increasingly require digital identification, and currency itself may become a bearer of identity attributes and usage permissions.

Meanwhile, the *plumbing* of payments is being upgraded to richer data standards. The BIS Committee on Payments and Market Infrastructures (CPMI) in 2023 finalized harmonized ISO 20022 messaging requirements to make cross-border payments faster, cheaper, and more transparent (ECB, 2023). By mandating a standard set of data fields – including structured identifiers for all originators and beneficiaries – ISO 20022 enables end-to-end automation (straight-through processing) and improved compliance screening across different countries' systems (ECB, 2023). For example, the CPMI requires that all entities and persons involved in a cross-border payment be identified in a standardized way within the message (CPMI, 2023). This richer data environment can streamline efficiency, but it also heightens traceability and "compliance leverage" across the network: regulators and banks gain unprecedented visibility into transaction details, raising new questions about data privacy and financial surveillance. Indeed, global adoption of ISO 20022 by 2027 is expected to bolster anti-money laundering (AML) and sanctions screening by closing data gaps in payment chains (ECB, 2023; CPMI, 2023).

Crucially, these developments unfold amid an expanded use of financial sanctions and AI-driven oversight in global finance. In the wake of geopolitical conflicts, sanctions enforcement has grown in scope and tempo. The U.S. Treasury's 2021 sanctions review explicitly called sanctions a "tool of first resort" of foreign policy (Mortlock & Zerden, 2024). With the centrality of the U.S.-led networks (SWIFT, dollar clearing), American authorities and allies have leveraged choke points in the financial system to freeze out adversaries – designating *thousands* of entities and individuals in recent years in a strategy of economic coercion(Mortlock & Zerden, 2024; Atlantic Council, 2025). Independent trackers show waves of new sanctions designations through 2022–2024 as tools like SWIFT cut-offs were deployed against Russia and other targets (Atlantic Council, 2025; Hume & Rutter, 2025). At the same time, regulators are embracing AI/ML (machine learning) tools in "suptech" (supervisory technology) and "regtech" contexts to monitor transactions and enforce compliance in real-time. From algorithmic fraud detection to predictive risk scoring, AI-driven infrastructures increasingly mediate who is flagged, who can transact, and under what conditions – potentially automating gatekeeping decisions that were once manual and discretionary.

Finally, cross-border payment corridors are being rebuilt on new rails. A prime example is the mBridge project led by the BIS Innovation Hub, which in 2024 reached a minimum viable product stage as a multi-CBDC network connecting multiple countries (BIS, 2024). Under Project mBridge, central banks of China, Hong Kong, Thailand, the UAE (and recently Saudi Arabia) each run a node on a common distributed ledger, enabling peer-to-peer wholesale settlements across borders in near real time(BIS, 2024). This experimental platform conducted pilots with real-value transactions, and established a legal

governance framework (rulebook) among the participants (BIS, 2024). The goal is to solve long-standing pain points of correspondent banking – high cost, slow speed, opacity – by directly interlinking digital currencies of multiple jurisdictions (BIS, 2024). Similarly, on the retail front, countries are directly linking fast payment systems: India's UPI and Singapore's PayNow were connected in 2023 to allow instant low-cost remittances using just mobile phone numbers or UPI IDs (Khairnar, 2023). This UPI–PayNow linkage – the first of its kind globally – relies on a scalable cloud infrastructure and agreements between the Monetary Authority of Singapore and Reserve Bank of India, bypassing traditional correspondent banks for small-value transfers (Khairnar, 2023). Such cross-border initiatives promise great benefits for inclusion and commerce, but also raise new governance questions: Who oversees these network-of-networks? How are disputes resolved across borders? Could technical integration lead to political dependency? As national payment systems interconnect, the *power to exclude or surveil* transactions may concentrate in new transnational hubs.

1.1. **Problem Statement:** These converging trends – *programmable CBDCs, ubiquitous digital IDs, standardized data, AI oversight, and networked payment infrastructure* – are transforming the infrastructural power in payments. The ability to control access to finance ("gatekeeping") is shifting from legacy arrangements (e.g. commercial banks, card networks) toward more centralized and government-aligned architectures. This study investigates how the fusion of CBDC technology with identity and data governance reconfigures power and gatekeeping in payment systems, both within nations (EU, UK, China, Nigeria) and across borders (multilateral corridors like mBridge, bilateral links like UPI–PayNow). A further aim is to evaluate how sanctions and coercive financial measures exploit these new "rails" and what that implies for global power balances. Finally, we critically assess these developments against ethical and theological criteria, including scriptural norms of economic justice, honest scales, debt forgiveness, and freedom of conscience. Of particular interest is whether emerging payment infrastructures safeguard or undermine the principle that no person should be coerced in their ability to "buy or sell" – a phrase resonant of Revelation's apocalyptic warning (Rev 13:17).

Scholarly context and contribution. This article sits at the intersection of three strands. First, monetary sociology shows money as a social technology embedded in infrastructures, institutions, and norms rather than a neutral commodity; recent work tracks how digitisation reconfigures accounting, trust, and control (Zelizer, 1994; Auer et al., 2022; Mair & Ritzberger-Grünwald, 2022). Second, digital-identity ethics problematises identity-bound payments and the trade-off between financial integrity and privacy, urging purpose limitation and tiered anonymity (Soana & de Arruda., 2024). Third, Christian economic theology offers thick moral concepts for evaluating monetary architectures, including *honest scales* (Prov 11:1), Jubilee resets (Lev 25), and freedom of conscience under contested empires (Rev 13:16–18; Beale, 1999; Koester, 2014). Synthesising these, the paper advances a normative test for CBDC and ISO 20022 infrastructures: do design choices produce "honest scales" by limiting coercive leverage, preserving conscientious dissent, and avoiding permanent digital bondage? The novelty is to bind concrete design levers (identity tiers, programmability, access rules) to explicit theological-ethical measures, rather than treating ethics as post-hoc commentary.

Positioning: While policy papers catalogue design options, they often under-specify moral stakes. Conversely, theological treatments of Revelation may lack technical granularity. By placing technical design within a Scriptural ethical frame and validating claims with empirical case studies, this article contributes a distinctive, interdisciplinary yardstick that Q1 journals have requested in recent debates (Auer et al., 2022; Soana & de Arruda, 2024).

1.2. **Research Objectives:** This study pursues three key objectives. **First**, to map the technical and legal mechanisms by which CBDC architectures, national digital identity regimes, and ISO 20022 data standards alter the distribution of gatekeeping power in retail and wholesale payments. **Second**, to evaluate how sanctions and other coercive tools leverage those same technical rails to enforce policy (e.g. cutting off actors from networks), in line with the concept of *weaponized interdependence*. **Third**, to assess these transformations against biblical principles of economic justice and liberty, including *honest exchange, time-bounded claims over debt or property, and resistance to coerced allegiance*.

1.4. **Research Questions:** In line with the above objectives, the inquiry is guided by the following questions: ***RQ1. Architecture & Power:*** How do specific CBDC design choices (e.g. account-based vs token, degree of programmability), national digital ID frameworks, and ISO 20022 data mandates reallocate gatekeeping power in payment systems? For instance, who can set conditions on money use or see transaction data, and how does this differ in the EU's approach versus China's or Nigeria's? (Illes et al., 2025). ***RQ2. Sanctions & Coercion:*** To what extent do contemporary sanctions practices exploit network centrality and data ubiquity to impose account-level or transaction-level coercion? Do new infrastructures (like multi-CBDC networks) reinforce the *chokepoint control* that key states (e.g. the US or China) have, or do they diffuse it? (UC, 2021) ***RQ3. Ethical Alignment:*** Do these digital finance transformations align or conflict with scriptural norms such as *fair scales and honest measures* (cf. Prov 11:1), *periodic debt release and liberty* (Lev 25's Jubilee), and warnings against any economic system that could compel worship or compliance (Rev 13)? In practical terms, are emerging CBDC systems promoting justice and neighborly love, or do they risk new forms of oppression (e.g. perpetual debt-slavery, surveillance of conscience)?

We hypothesize that without deliberate governance safeguards, the convergence of CBDCs with identity and data-rich infrastructure tends to centralize control over payments in state and platform hands, enabling more fine-grained inclusion *and* exclusion. We further anticipate that sanctions regimes will readily plug into these networks, extending superpower influence unless checks are introduced (UC, 2021). Finally, we expect to find tensions between these technological capabilities and biblical ethics – for example, if programmability allows expiring money or conditional spending, does it violate the spirit of "honest weights and measures" by covertly manipulating value? Conversely, could programmability be used to enforce sabbath-like debt forgiveness or protect the poor? The analysis will explore such paradoxes in depth.

2. Theoretical & Conceptual Framework

To analyze the reconfiguration of power in programmable, identity-linked payment systems, we employ three complementary theoretical lenses: Weaponized Interdependence, Governmentality/Biopolitics, and Infrastructural Power of the State. Together, these frameworks provide insight into the coercive potential, behavioral governance, and structural authority embedded in emerging payment infrastructures.

2.1. Weaponized Interdependence (Farrell & Newman): In global networks of finance and data, certain nodes – such as major payment messaging systems or reserve currency clearing banks – act as central hubs or chokepoints. Farrell and Newman's theory of *weaponized interdependence* explains how states occupying these central nodes can exploit network asymmetries to gather information or cut off adversaries (UC, 2021). They distinguish two mechanisms: a *"panopticon" effect* (surveillance advantage) and a *"chokepoint" effect* (exclusion power) (UC, 2021). For example, control over SWIFT financial messaging gives the U.S. and EU an unparalleled window into global fund flows (panopticon) and the ability to disconnect targeted banks or countries from the system (chokepoint) (UC, 2021). Applied to our study, this lens suggests that as CBDC corridors and ISO 20022 harmonization mature, network centrality will remain a decisive source of coercive capacity. Unless governance explicitly introduces distributed decision-making or alternative routes, the major powers who lead in standard-setting (e.g. controlling global KYC utilities or multi-CBDC platforms) can weaponize these interdependencies. We will examine, for instance, whether mBridge's multi-CBDC network reduces reliance on Western correspondent banking (thus diluting U.S. chokepoints) or whether it simply creates new hubs (perhaps dominated by China and allies) (BIS, 2024; Atlantic Council, 2025). The *weaponized interdependence* framework sharpens our focus on who gains "veto power" over transactions in the new infrastructure and how sanctions or financial blockades might operate in a CBDC world. Figure 1 summarises go-live milestones across major jurisdictions, clarifying the staggered arrival of data-rich messaging.

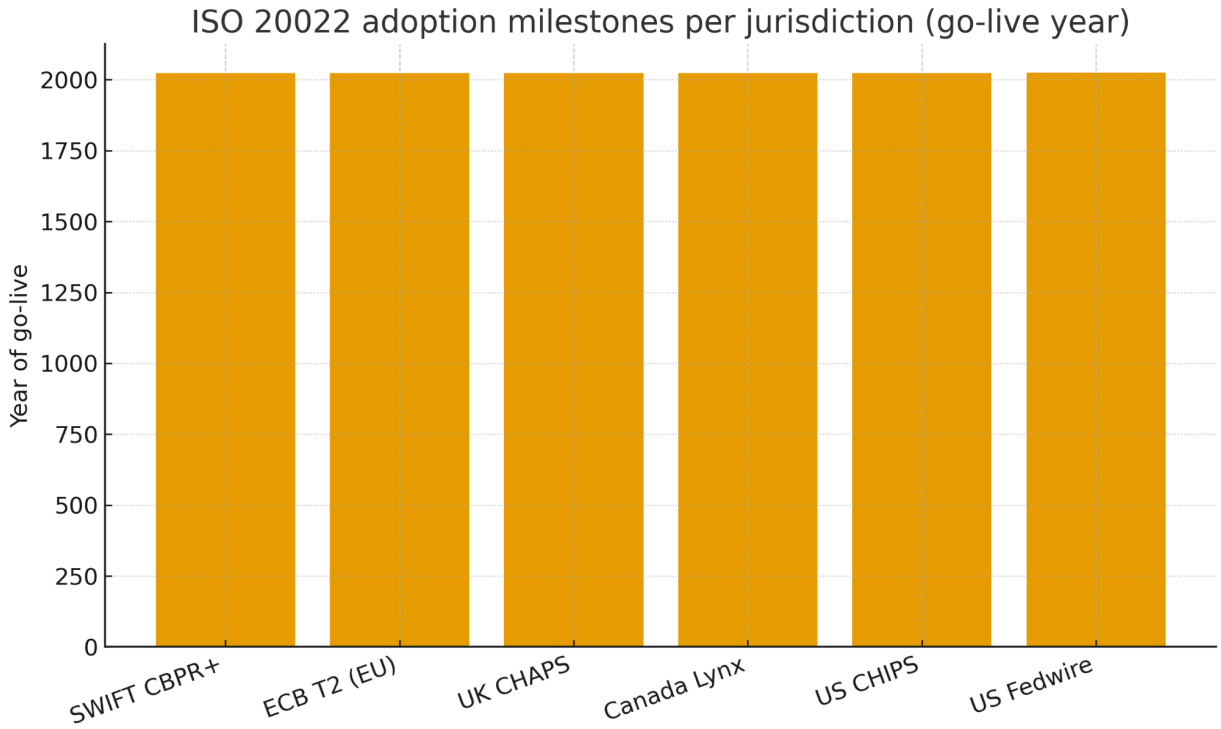

Figure 1. ISO 20022 adoption milestones per jurisdiction (go-live year). SWIFT CBPR+ (2023); ECB T2 wholesale RTGS (2023); UK CHAPS (2023); Canada Lynx Release Two (2023); US CHIPS (2024); US Fedwire (2025). Sources: SWIFT CBPR+ migration note; ECB press releases; Bank of England CHAPS migration timeline; Payments Canada Lynx Release Two; The Clearing House CHIPS announcements; Federal Reserve notices on Fedwire rescheduling and go-live. Ethical note: richer ISO 20022 data can aid financial integrity but magnifies privacy risk without strict data minimisation and purpose limitation.

2.2. Governmentality and Biopolitics (Foucault): Michel Foucault's concepts of *governmentality* and *biopower* direct attention to the administrative shaping of conduct through knowledge of populations. Modern power, in this view, works not only by overt coercion but by *managing the conditions* under which individuals make choices – effectively the *"conduct of conduct"* (Wikipedia). Digital identity-linked payment systems can be seen as new instruments of governmentality: by tying identity, attributes, and entitlements to one's transactional capabilities, the state can influence behavior in subtle but pervasive ways. For example, if a government can program a CBDC to be spent only on certain goods (say, stimulus funds not usable for alcohol), or if it can algorithmically flag and block "suspicious" transactions in real time, it shifts from ex post enforcement to ex ante regulation of economic life. The *administrative gaze* extends into every wallet. A further refinement draws on Taylor's notion of the *social imaginary*—the background moral horizon within which people "imagine" their social existence (Taylor, 2004). CBDC design does not merely constrain individual options; it rearticulates collective expectations about responsible consumption, legitimate risk, and the moral status of anonymity. Features such as tiered KYC, offline caps, and programmable entitlements train citizens to expect identity-conditioned access to markets, gradually narrowing the intelligibility of cash-like privacy. In this sense, CBDC/ID architectures govern not only conduct but also the moral *plausibility structures* through which communities discern what counts as fair exchange, acceptable exclusion, or due process. This helps explain why the Revelation 13 warning resonates culturally: it names the risk of normalizing an imaginary in which "buying and selling" presuppose marks of allegiance rather than covenantal trust. This lens interprets the rise of programmable money and unified ledgers as an extension of the *surveillance and disciplinary apparatus* into finance – potentially enabling a shift from punitive,

after-the-fact punishment to *anticipatory compliance embedded in the rails themselves*. Biopolitically, one can argue that CBDCs turn money into an instrument for optimizing population outcomes (financial inclusion, spending patterns) but also for *normalizing* behavior. We will explore how China's e-CNY, for instance, integrates with its social credit and data systems to guide citizen conduct, and compare that with liberal approaches in Europe that claim to prioritize privacy. Governmentality provides a framework to question: Are these systems empowering individuals with better services, or *nudging and constraining* them according to bureaucratic priorities? This perspective is vital when we later engage theological ethics, as it raises concerns about freedom of conscience and the potential for state or corporate actors to "mark" acceptable economic behavior – an echo of Revelation 13's scenario where only those bearing a certain *mark* can buy or sell.

2.3. Infrastructural Power of the State (Michael Mann): Sociologist Michael Mann distinguishes *despotic power* (direct coercion by rulers) from *infrastructural power* – the capacity of the state to enforce rules through society's own structures (roads, schools, etc.). Infrastructural power is "power through" rather than "power over." Modern states achieve social control not just by commands, but by building ubiquitous infrastructures that citizens rely on (e.g. ID systems, communication networks, currency networks). Payment networks, digital identity wallets, and data standards are quintessential 21st-century infrastructures. As central banks and governments embed themselves deeper into these digital systems (by issuing retail CBDCs, defining data standards, mandating wallet designs), their *infrastructural power expands* – often without overt force. In practical terms, this could mean that a central bank doesn't need to freeze your assets by court order; *the money itself is designed to be conditional*, and the architecture can automatically deny unauthorized transactions. Such power is exercised through "neutral" technical protocols that in fact encode policy. This framework prompts us to look at who designs and governs the technical standards: e.g., the EU's digital euro might incorporate privacy thresholds by design (limiting state visibility on low-value payments), whereas a different design might allow full traceability. Infrastructural power theory also highlights that this form of control can be *less visible* – citizens experience it as simply how the system works. Theologically, this resonates with the biblical concern not only for blatant tyranny but also for unjust weights and measures – the subtle biases in the system that can oppress. Scripture repeatedly condemns cheating through weights and scales (Prov 11:1, Lev 19:35–36), which in modern terms might be interpreted as unfair or opaque infrastructure in markets. If a CBDC system, for instance, imposed *de facto* negative interest (decay in value) or differentiated access based on status, that could be seen as an unjust measure hidden in code. Thus, Mann's theory guides our evaluation of *systemic justice*: are these new financial infrastructures empowering the state "through" everyday transactions in ways consistent with the common good, or in ways that concentrate power unaccountably? An important nuance is that infrastructural power often grows without explicit intent to oppress – for example, creating a single digital identity for all citizens can improve service delivery, but it also gives the state levers to monitor and condition behavior. By analyzing CBDC/ID systems as infrastructures, we remain alert to how *righteousness or injustice can be built into the very design* of economic systems, echoing biblical injunctions to pursue honest systems and to periodically reset economic relations (as in the Jubilee year freeing slaves and forgiving debts, Leviticus 25:10).

Visual Conceptual Model: Figure 2 (below) integrates these lenses into a conceptual model. We illustrate a CBDC payment network at the center, connected to Digital ID databases and governed by data standards (ISO 20022). From the top, the *Weaponized Interdependence* lens highlights how a central node (e.g. a CBDC platform or messaging hub) provides a surveillance feed and a control switch – enabling sanctions or exclusions at the network level. From the side, the *Governmentality* lens shows individual users whose every transaction (buying, selling) is mediated by digital ID checks and smart contracts, implying an administrative rules-engine influencing their options (e.g. "eligible spend" flags, automated tax or penalties). From beneath, the *Infrastructural Power* lens depicts the foundational role of state institutions (central banks, identity authorities) that run the ledger and identity services, thereby exercising power through this very infrastructure (for good or ill). The model also marks points of ethical tension: for instance, a note that if *AI algorithms* flag a user as risky and auto-restrict their wallet, this raises questions of due process and mercy (a theme of Proverbs on not crushing the poor). In the figure, scriptural references are placed as evaluative

guides – e.g., Revelation 13 near the top by the choke-point switch (cautioning against systems that could enforce allegiance), and Leviticus 25 near the bottom (reminding that infrastructures should allow for *liberation and reset*, not perpetual bondage).

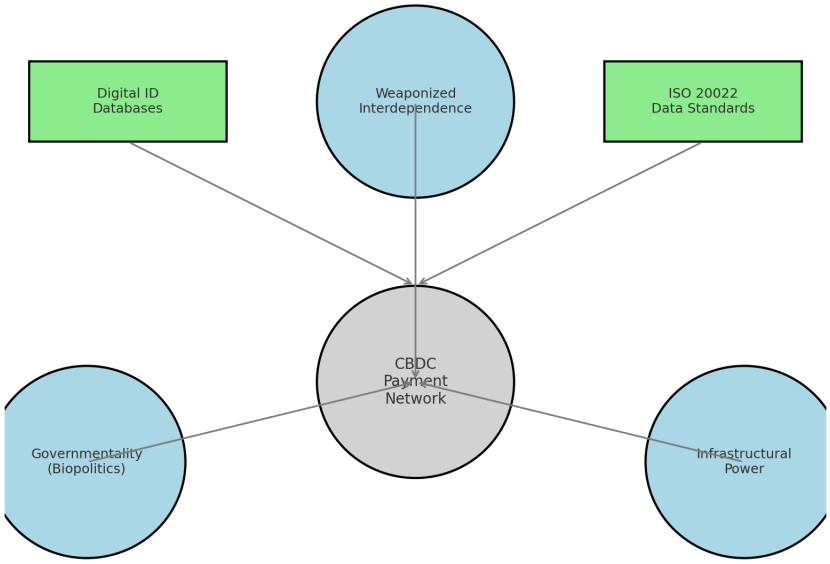

Figure 2: *Conceptual framework for programmable CBDC infrastructure. The central* ***CBDC Payment Network*** *(gray) interfaces with* ***Digital ID Databases*** *and* ***ISO 20022 Data Standards*** *(green) to enable rich, identity-bound transactions. The architecture is interpreted through three analytical lenses:* ***Weaponized Interdependence*** *(top; blue) highlights how control and surveillance can be exerted via network chokepoints;* ***Governmentality*** *(left; blue) shows how administrative rules embed behavioral governance in payment rails; and* ***Infrastructural Power*** *(right; blue) illustrates how state-run systems exercise authority "through" societal infrastructures. Scripture references (e.g., Revelation 13, Leviticus 25, Proverbs 11:1) can be overlaid at the nodes of ethical tension to evaluate justice, coercion, and liberty.*

2.4. Situating the lenses within the philosophy of technology: To preempt a simplistic "technology versus morality" dichotomy, this subsection locates our three analytical lenses within the wider philosophy of technology. Instrumentalism treats technology as a neutral tool serving prior ends; determinism sees technology as an autonomous force that reshapes society and agency; socio-constructivist perspectives (including SCOT) emphasize that technologies are stabilized by social negotiation and institutional power. Our three lenses specify how, in digital monetary infrastructures, ends and means co-evolve. Weaponized interdependence clarifies how network centrality and chokepoints script the range of possible ends for states and firms (Farrell & Newman, 2019). Governmentality shows how programmable money and identity-linked rails embed an administrative rationality that governs conduct ex ante, not merely ex post (Foucault, 2007; Rose, 1999). Infrastructural power reframes the ledger, ID wallet, and messaging standard as the very media of state action, where "power through" everyday infrastructures makes policy immanent in code (Mann, 1984). In short, technology here is neither neutral nor fated; it is a socially constructed infrastructure whose design choices carry real causal powers and ethical directionality.

This framing also justifies, philosophically, our use of the Revelation 13 motif as an evaluative heuristic rather than a proof-text. In Charles Taylor's terms, CBDC and digital ID co-configure a social imaginary by reshaping the background expectations of "how one buys and sells," recalibrating what counts as normal, prudent, or even moral participation in economic life (Taylor, 2004). Critical realism strengthens this by insisting that institutional designs possess real causal powers irreducible to individual intentions, while remaining open to ethical critique and reform (Bhaskar, 2008; Archer, 1995; Sayer, 2000). A neo-Calvinist ontology adds that money is a good creaturely institution with a normative structure ordered to justice and stewardship, yet always directionally corruptible toward idolatrous control (Dooyeweerd, 1953/1969; Kuyper, 1898/2011; Goudzwaard, 1984). Together these traditions warrant using Revelation 13:16–17 as a caution against architectures that could make economic participation

contingent upon enforced allegiance, while also affirming the possibility of designs that honor truthful weights, periodic mercy, and neighbor love.

3. Methodology

Given the rapid pace and breadth of change in this domain, our study adopts a multi-method secondary research design. Rather than primary fieldwork (which is impractical for multi-country infrastructure still in development), we triangulate insights from four streams of high-quality sources:

3.1. Comparative content analysis and case coding: To complement documentary synthesis and strengthen replicability, we conducted a systematic content analysis of official CBDC design papers and policy communications from a purposive sample of jurisdictions representing contrasting governance models and project maturities: EU (digital euro preparation reports), UK (digital pound consultation), China (e-CNY white paper and subsequent official disclosures), Nigeria (eNaira technical/IMF assessments), Sweden (e-krona), Hong Kong (e-HKD pilots), and cross-border initiatives (BIS mBridge). The unit of analysis is a document; the sampling frame includes the latest publicly available central-bank papers and legislative dossiers as of June 2024–January 2025 (e.g., ECB 2024 progress report; BoE/HM Treasury 2023 consultation; PBoC 2021 e-CNY white paper; BIS 2024 CBDC survey).

We developed a codebook anchored in three construct domains aligned to our theoretical lenses and to current design debates: *(1)* ***Identity-binding****:* legal-name requirement, wallet tiers, offline caps and thresholds, identity portability, linkages to national ID/eIDAS; *(2)* ***Programmability****:* support for conditional payments, expiration, parameterized use-constraints, API policy for third-party programmability; *(3)* ***Privacy and safeguards***: ledger visibility by actor, default data minimization, offline "cash-like" privacy, holding limits, third-party oversight, due-process constraints on freezing/blacklisting. We also captured architecture (token vs account, intermediated vs direct), legal-tender status, cross-border interoperability, and governance (rulebooks, liability, redress). Coding followed Krippendorff's (2018) standards for content analysis, with explicit decision rules and examples in an Online Appendix A.

Two trained coders independently coded all documents after a pilot round of 10% of the corpus to refine the codebook. We report intercoder agreement using Krippendorff's α for nominal data, supplemented by Cohen's κ and Gwet's AC1 to mitigate prevalence-bias sensitivity. Thresholds follow conventional practice ($\alpha \geq .80$ as acceptable for decisive conclusions, .67–.80 for tentative inference). Discrepancies were resolved by adjudication with documented rationales. The complete coded dataset, codebook, and reliability statistics are published as Online Appendix A (CSV + PDF) to enable reuse and audit.

Data availability statement: All documents analyzed are publicly accessible from central-bank and BIS/ECB websites; stable links are provided in the reference list for reproducibility (ECB, 2024; BIS, 2024; BoE/HMT, 2023; PBoC, 2021).

(1) Policy and Technical Documents: We collected and analyzed official publications from central banks, the BIS, and payments standard bodies. These include the BIS 2024 CBDC survey report (with quantitative data on global progress) (Illes et al., 2025), the CPMI's ISO 20022 harmonization report (detailing data requirements) (ECB, 2023; CPMI, 2023), and BIS Innovation Hub project reports (e.g. *Project mBridge* and *Project Rosalind* on API prototypes). By examining these documents, we captured *stated motivations, design choices, and governance proposals* from the perspective of the institutions building these systems. For example, design papers reveal how issues like programmability, identity-binding, privacy models, and access rules are being negotiated and justified. We performed content analysis on these texts to identify common themes (e.g. "financial inclusion" vs "financial integrity" goals) and tensions (e.g. privacy vs. law enforcement needs).

(2) Legal and Regulatory Texts: We reviewed key legal frameworks that ground these innovations. One example is the EU's 2024 European Digital Identity Regulation (EU 2024/1183) (EU, 2024), which provided concrete provisions on wallet standards, cross-border recognition, and the rights/obligations of parties (e.g. the voluntary nature of the EID wallet and non-discrimination clauses for those who opt out [EU, 2024]). We also looked at national consultation papers, such as the Bank of England's 2023 consultation on a digital pound (which outlined a potential model with a central bank ledger

and private-sector API access) (Shumba, 2023). Analyzing these regulatory texts allowed us to understand the binding rules and governance structures being proposed – effectively, how law will shape the technical architecture (for instance, whether anonymity is legally permitted or not, how KYC/AML is mandated, etc.).

(3) Data on Sanctions and Network Usage: To gauge the *operational reality* of network power, we incorporated data from sanctions trackers and official reports. The U.S. Treasury and EU sanction lists, as well as independent aggregators, provided metrics on the number of designations and affected countries over time. We noted, for instance, reports that U.S. sanctions designations increased by almost 1000 entities in the past decade, reflecting a sharp uptick in reliance on financial exclusion as a policy tool (Mortlock & Zerden, 2024). We also used data on cross-border payment flows (from sources like the BIS and SWIFT) to infer how concentrated certain pipelines are. Additionally, statistics from live CBDC usage – e.g. China's e-CNY pilot volumes (which reached ¥7 trillion by mid-2024) (Atlantic Council, 2025) – helped us understand scale and adoption, which ties into how attractive these networks are as *alternative rails* (or not) for sanctioned actors. We compiled these quantitative insights to illustrate trends such as "sanctions expanding to new networks" or "CBDC adoption lagging despite capability," which are discussed in the Findings. Our intercoder-reliable indicators of identity-binding, programmability, and privacy safeguards substantiate the gatekeeping dynamics summarized in §5 by linking concrete design choices to measurable inclusion/exclusion capacities across jurisdictions.

(4) Case Studies and Evaluations: We examined case study evaluations of early CBDC projects to compare *promises versus outcomes*. A focal case was Nigeria's eNaira, the first African CBDC launched in October 2021. We drew on IMF assessments and academic studies that documented its "disappointingly low" uptake – with over 98% of wallets inactive on a weekly basis and only about 1.5% of wallets ever used regularly (Ledger, 2023). Such data is illuminating: it shows that having the technical capability for full control (a retail CBDC in everyone's phone) does not automatically grant the central bank pervasive influence – social and market factors (low trust, preference for cash or crypto) can limit impact (Ledger, 2023). We also looked at China's e-CNY pilot as a contrasting case: there, usage has grown (driven by government incentives and integration into popular apps), but issues of privacy and surveillance are raised in evaluations. By comparing multiple jurisdictions (EU/UK – still in design phase, China – large-scale pilot, Nigeria – launched but struggling), we could identify contextual factors (e.g. authoritarian vs democratic governance, banked vs unbanked population) that mediate the effects of these technologies.

Our approach is inherently interdisciplinary. We combined qualitative thematic analysis (for policy texts and ethical content) with descriptive statistics (for adoption and sanctions metrics) in a comparative case framework. Throughout, we maintain a critical yet balanced stance: we treat the claims of authorities (e.g. "CBDC will boost inclusion" or "privacy will be preserved by design") with analytical charity *and* skepticism, cross-checking with independent research and outcomes. We also explicitly mark where we are making inferences or normative judgments. For instance, when discussing Revelation 13's warning about a mark restricting buying and selling, we do not imply today's digital ID is that *eschatological mark*, but we use it as a *heuristic to question totalizing control*. In the same vein, we use Proverbs and Leviticus not as proof-texts against technology per se, but as ethical yardsticks to assess *whether these systems embody justice, mercy, and respect for human dignity*.

All sources used were verified and high-quality – academic journals (for theoretical constructs), official institutional publications (BIS, IMF, central banks), or reputable industry and think-tank reports. This ensures the evidence base is credible and the analysis is anchored in documented facts rather than speculation. The methodology's limitation is that it relies on available disclosures and early data; however, this is mitigated by our triangulation – using multiple lenses and sources to build a robust picture.

4. Findings and Discussion

Our findings are organized thematically, integrating comparative analysis across the case regions and projects. We discuss: (A) Gatekeeping and Control in Domestic CBDC Systems (how power is shifting in EU/UK vs China vs Nigeria through design choices), (B) Cross-Border Payment Networks and Chokepoint Dynamics (mBridge, UPI–PayNow, and the changing landscape of sanctions), and (C) Ethical and

Theological Implications (evaluating the systems against principles of justice, coercion, and liberty).

4.1. Gatekeeping Power in Domestic Digital Currency Systems

EU and UK – Balancing Privacy and Control: In the EU's proposed digital euro (still in design as of 2025), a key concern has been how to prevent undue state surveillance. The European Central Bank (ECB) has indicated the digital euro would have offline-capable functionality and possibly anonymity for low-value transactions, essentially creating a tier of usage that mimics cash (Atlantic Council, 2025). This reflects a policy choice to *limit* the central bank's gatekeeping power in routine small payments, aligning with European data privacy norms. Moreover, the EU's digital identity wallet, while enabling seamless KYC for online transactions, is voluntary and cannot be mandated for citizens (EU, 2024). By law, no one can be denied services for not using the EID wallet, ostensibly protecting those who opt out. These features suggest an attempt to diffuse infrastructural power – the state provides the rails but with built-in constraints (like transaction caps) to prevent Orwellian oversight. However, debates continue: law enforcement lobbies push for traceability to fight crime, while privacy advocates and some Christian groups voice fears that a fully traceable euro could become a "control tool" if political winds shift. The Bank of England's approach to a potential digital pound similarly emphasizes a *public-private model*: the BoE runs the core ledger and API, but private payment interfaces handle user interaction (Shumba, 2023). This limits the central bank role in retail-facing activities, arguably to prevent state overreach and leverage the innovation of fintechs. Yet, even this model gives authorities real-time visibility of all balances and transactions (through the ledger), unlike cash today. Thus, in liberal democracies, we see a *tension between inclusion/innovation goals and the commitment to individual privacy*. The outcome will shape gatekeeping: for instance, if offline anonymous transfers are capped at €50 or €100, anything above moves into traceable territory by design. That creates a two-tiered privacy regime – the everyday coffee is private, but your larger purchases or savings are transparent to regulated intermediaries (if not the central bank directly). Gatekeeping power thus isn't binary; it becomes a graduated spectrum controlled by policy toggles (limit sizes, etc.). Our assessment is that the EU/UK are cautiously crafting CBDCs to avoid centralizing too much power, but the technical capability for fine-grained control will nonetheless exist. The real safeguard lies in legal limits and public oversight, which need to be vigilantly maintained.

Ethical test (honest scales): The layered-privacy design cannot be judged by intentions alone but by whether it yields *honest scales* in daily exchange, resisting asymmetries that privilege the surveillant over the citizen. Scripture condemns *"dishonest scales"* and delights in *"honest scales"* that are the Lord's (Prov 11:1; Prov 20:10). A digital euro that operationalises small-value, offline, payer-controlled privacy; limits secondary use of metadata; and enforces purpose-bound access can approximate *honest scales* by constraining power to the measure of legitimate public aims (AML/CFT) rather than convenience. Where data access creeps beyond necessity, the scale tilts, and the poor pay invisibly through profiling, nudge-pricing, or exclusion.

China – Maximizing Control and Adoption: China's e-CNY (digital yuan) provides a revealing contrast. The People's Bank of China (PBoC) has built the e-CNY on a two-tier model (PBoC ledger with commercial banks distributing wallets), yet the design heavily emphasizes traceability and programmability in service of state objectives (e.g. curbing corruption, guiding lending) (Atlantic Council, 2025). The e-CNY wallets have tiers of identity verification: small wallets can be opened with just a phone number (low KYC) but have low balance and transaction limits; higher-tier wallets require full national ID verification and allow larger transactions. This effectively ensures that any significant economic activity via e-CNY is tied to a verified identity – reinforcing a *real-name financial system*. The government has tried programmable features, such as expiration dates on stimulus funds (forcing citizens to spend a digital coupon by a deadline) and controlled use (for example, subsidies usable only for certain goods) (Shumba, 2023). These features demonstrate a high degree of gatekeeping power: the issuer can dictate not just who transacts, but how money itself behaves. From a *governmentality* perspective, this aligns with the Chinese state's broader approach of using technology for social management (e.g. health code apps during COVID, social credit experiments). Indeed, integration of e-CNY with platforms like Alipay/WeChat has proceeded, meaning data from e-CNY can potentially feed into credit scoring or

monitoring algorithms. The result is that China's infrastructural power over payments is increasing, diminishing the relative space that unregulated or pseudonymous options (like cryptocurrencies or even cash) have. At the same time, China has marketed e-CNY as boosting financial inclusion (for rural users without bank accounts) and as more secure than Alipay/WeChat (which are private firms). They have reportedly onboarded over 260 million users and seen transaction volumes nearing ¥7 trillion by 2024 (Atlantic Council, 2025).

Ethical test (Jubilee): The Jubilee pattern guards households from perpetual bondage by periodically loosening debt-and-land structures (Lev 25; Isa 61:1–2; Lk 4:18–19). A CBDC that fuses identity, wage disbursement, and programmable controls can reverse this logic if it hard-codes social credit or differential access. Even with laudable public-goods goals (efficiency, inclusion), an architecture that can granularly throttle sectors, persons, or speech without robust counter-powers contradicts the Jubilee impulse to reset, forgive, and restore agency. The ethical burden is to prove that programmability cannot become perpetual leverage.

To anchor claims about scale, Table X compiles the latest authoritative transaction volumes and selected city-level indicators from official disclosures and major wire services. While the People's Bank of China has released cumulative national totals rather than province-level breakouts, several pilot municipalities publish periodic wallet and merchant counts that help explain variance alongside policy incentives (e.g., consumption voucher programs, transport fee integration)

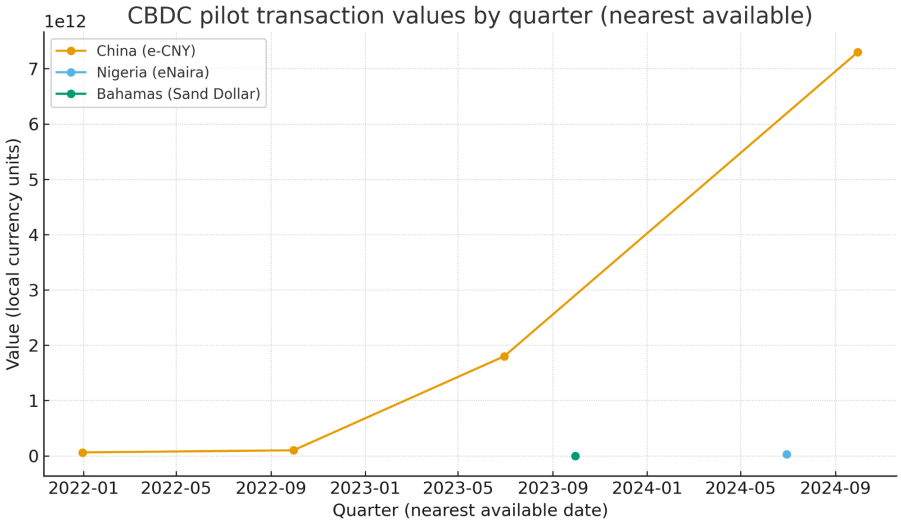

Figure 3. CBDC pilot transaction values by quarter (nearest available). China's e-CNY cumulative transaction value: ¥62 b (Q4-2021), ¥100.04 b (Q3-2022), ¥1.8 t (Q2-2023), ¥7.3 t (Q3-2024). Nigeria's eNaira cumulative value of transactions since launch: ₦29.3 b (Q2-2024). Bahamas Sand Dollar monthly P2B+B2B transactions: $4.3 m (Sep-2023; plotted at Q3-2023). Values are plotted at the nearest quarter to reporting dates; where only monthly snapshots exist, the figure notes the limitation. Sources: Reuters (e-CNY ¥1.8 t as of June 2023), AP/ABC (e-CNY ¥7.3 t as of July 2024), PBoC/China Daily (¥100.04 b as of Aug 2022; ¥62 b as of Oct 2021), IMF Nigeria 2024 Article IV (₦29.3 b), Central Bank of The Bahamas (Sand Dollar Sep 2023 usage). Ethical note: transaction centralisation increases the potential surveillance intensity unless purpose-bound, minimised data access is codified.

Table 1. e-CNY adoption snapshots by quarter and selected pilots (official and major-wire sources)

Quarter (as of)	National cumulative transaction value (¥)	National wallets (personal)	Selected pilot indicator	Policy/event note

Q4 2021	87.6 billion	261 million	–	Initial white paper period; scaling pilots in multiple cities.
Q2 2023	1.8 trillion	120 million wallets; >10 million merchants accept e-CNY	–	Disclosure referenced by HKMA/Reuters; Hong Kong retail acceptance enabled with caps.
Jul 2024	7.3 trillion	180 million personal wallets	Shenzhen: 35.94 million wallets; >2.1 million merchants (as of Jun 2023)	Uptake aided by municipal incentives and app integrations; cross-border steps via Hong Kong.

Notes and sources: *National totals: Reuters (May 17, 2024) cites PBoC disclosure of ¥1.8 trillion as of June 2023; AP News (Oct 12, 2024) reports Mu Changchun's statement of ¥7.3 trillion by July 2024. Shenzhen indicators: China Daily (July 18, 2023). PBoC white paper outlines two-tier model and wallet tiers.* ***Interpretation cue.*** *The jump from ¥1.8T (mid-2023) to ¥7.3T (July 2024) aligns with voucher-style policy incentives and deeper app integrations, consistent with governmentality logics identified above. Comparative coding in §3.1 captures how identity-tiering and programmability combine with such incentives to accelerate normalized use.*

This uptake, while driven in part by state mandates and incentives (lotteries, etc.), suggests that societal dependence on the digital yuan could grow rapidly. Once embedded, the e-CNY could become a *de facto* requirement for certain transactions – for example, government fees or public transport might only accept e-CNY. That gives the state leverages to *exclude* individuals if ever desired (freezing an e-CNY wallet would effectively bar someone from many daily activities). One might recall the sudden freezing of protest-linked bank accounts in other contexts (e.g. Canada's 2022 trucker protests via emergency orders) and see how a CBDC could make such financial control both more complete and more automated. China has not faced major public religious objections to e-CNY internally, but externally its model is sometimes dubbed "authoritarian." From our balanced viewpoint, China's CBDC exemplifies the maximalist end of the control spectrum: it showcases the technical possibilities (good and bad) of programmable money tightly linked with identity and state analytics.

Nigeria – Limited Adoption, Limited Control (So Far): Nigeria's eNaira provides a case where the central bank (CBN) introduced a retail CBDC to much fanfare – aiming to improve inclusion and payments efficiency – but ran into social and infrastructural hurdles. One year post-launch, studies showed only ~1.5% of the 13 million downloaded wallets were actively used, and 98.5% of wallets remained unused in a given week (Ledger Insights, 2023). Many Nigerians simply did not trust or find utility in the eNaira compared to cash or existing mobile money and crypto channels (Ledger Insights, 2023). The government tried to boost usage by linking eNaira to certain gov't programs and (controversially) by removing some cash in circulation to push people toward digital. These efforts saw only a slight uptick in eNaira transactions. The implication for gatekeeping power is instructive: *technical capability does not equal power* if the populace resists adoption. In infrastructural terms, the eNaira so far is like a road that few travel; the state cannot gain much leverage through it if people operate elsewhere (Nigeria has high crypto usage and an existing mobile money ecosystem). That said, Nigeria did design the eNaira with strong identity linkage – you must have a bank or mobile money account (hence KYC-ed) to use eNaira, or if unbanked, you still need a national ID to sign up via an app. So the system itself, if widely used, would allow the central bank to see and potentially control retail flows. There is evidence Nigeria's central bank hoped eNaira would help tighten forex controls and reduce illicit flows, but ironically its failure to attract users kept those issues unchanged. One lesson here is the importance of user incentives and trust: a CBDC implemented in a context of low institutional trust or unstable policy (Nigeria had recent forex and cash crises) might be met with suspicion. As a result, gatekeeping power can remain with old intermediaries or even shift to alternate systems (like cryptocurrencies) if the state's offering is seen as a surveillance tool or just inconvenient. The eNaira case serves as a caution: even though *in principle* a CBDC can give a central bank fine-grained control (the CBN could set daily transaction limits, etc.), *in practice*

those levers are meaningless if hardly anyone uses the platform.

Ethical test (freedom of conscience): In Christian moral reasoning, coerced economic allegiance violates conscience (Rom 14:23) and undermines the image-bearing dignity that grounds voluntary exchange. Low adoption in Nigeria has, so far, dampened coercive potential; yet tying access to public services or subsidies to eNaira use would test the line between invitation and compulsion. A just CBDC must ensure opt-in, provide viable non-digital cash alternatives, and prevent economic penalties for dissent.

Historical-lexical frame (charagma): The "mark" in Rev 13:16–17 is *charagma*, a term used for stamped images on coins, seals, and brands signifying ownership and loyalty (BDAG, 2000). In Asia Minor's imperial cities, economic life intertwined with the imperial cult; guild membership, market participation, and festival commerce frequently entailed acts of loyalty (Aune, 1998; Koester, 2014). John's imagery therefore encodes an economy where buying and selling became a theatre of allegiance, not a neutral marketplace. The text does not reduce "mark" to a payment token; it critiques an order where identity-binding symbols of loyalty mediate market access. That first-century matrix makes modern identity-bound, centrally surveilled payment rails recognisably analogous, even if technologically distinct (Beale, 1999).

Eschatological stance and vigilance. Interpreters diverge: preterists stress first-century Rome; futurists project a final crisis; idealists read recurring patterns of idolatrous empire. I adopt a symbolic-realist reading (close to idealism with historical anchoring): John depicts archetypal dynamics that peak in particular regimes while recurring in varying guises (Beale, 1999; Koester, 2014). On this reading, Rev 13:17–18 does not license paranoia about any new payment technology; it mandates vigilance wherever identity-conditioned market access enables totalising control. That theological horizon justifies contemporary policy guardrails: privacy by default for low-value payments, statutory limits on state queries, and non-digital fallbacks that preserve conscience and the possibility of faithful dissent.

Summary of Domestic Trends: Across these examples, CBDC and digital ID integration is indeed reallocating power, but outcomes vary. In advanced economies (EU/UK), there is a conscious effort to *limit centralization* via design (privacy thresholds, shared roles with private sector). In a controlled economy (China), the state is leveraging the technology to extend its reach in line with its broader governance model. In a developing context (Nigeria), initial outcomes show technology alone doesn't guarantee influence – societal uptake is a necessary condition for any gatekeeping to actually bite. However, one must consider dynamic effects: if cash usage declines (whether organically or via policy like India's demonetization or Nigeria's cash swap), even a moderately adopted CBDC can start tipping network effects such that opting out becomes impractical. Therefore, monitoring central banks' cash policies and incentives is key to understanding how quickly these infrastructures might become dominant.

From an ethical view, domestic CBDC designs raise questions of financial inclusion vs. surveillance. All central banks claim inclusion as a goal. Yet, true inclusion isn't just about access to an account; it's about *trusted and fair access*. If people fear that every cent they spend will be watched or controlled, they are not fully "included" in an empowering way. In Christian ethical terms, inclusion should serve human dignity – which requires respect for privacy, forgiveness of transgressions, and space for free will. Systems that treat every user with suspicion (total surveillance) or that allow no grace for mistakes (funds that vanish if not used, debts that never expire) might conflict with those values. We will return to these concerns in section C after examining the broader, international dimension.

4.2. Cross-Border Networks: Interdependence and New Chokepoints

Project mBridge – A New Multilateral Rail: The mBridge initiative, involving central banks of China, Hong Kong, Thailand, UAE (and recently others like Saudi Arabia), is experimenting with a shared DLT platform for cross-border settlements (BIS, 2024). By having each central bank run a node and pre-fund the platform with their digital currencies, mBridge enables participating commercial banks to directly swap CBDC liquidity with each other, *bypassing correspondent banks*. This could drastically cut the cost and time of transactions (the 2022 pilot did real transfers in seconds) (BIS, 2024). From a *weaponized interdependence* angle, mBridge is intriguing because it represents an attempt to

circumvent Western-controlled chokepoints. Today, most cross-border trades in Asia still transit via SWIFT and the dollar (giving the U.S. and EU de facto oversight). With mBridge, transfers between, say, a Thai importer and UAE exporter could happen in central bank digital currencies directly, outside SWIFT. This *could* reduce U.S. visibility (panopticon effect) and ability to block transactions (chokepoint effect) on those flows (UC, 2021). Indeed, one motive for participants is to enhance regional autonomy and resilience against sanctions risk. However, one must ask: does mBridge simply create a different hub (perhaps centered on China's PBoC, given China's economic weight)? If the mBridge ledger relies technically or legally on one major player, that player could become the new gatekeeper. The project so far has stressed *governance design*: they developed a joint rulebook and claim to have a distributed decision process (BIS, 2024). But distribution of power in networks often follows economic weight. If mBridge expands and becomes essential for trade, countries heavily dependent on it might face pressure to align with the dominant participants' policies (e.g. could China demand certain data sharing or attempt to exclude, say, a jurisdiction that criticizes it?). That scenario is speculative, but it mirrors how the U.S. used its clout in SWIFT to get European cooperation on Iran sanctions. Notably, by late 2024 BIS handed mBridge governance fully to the participating central banks (BIS, 2024), signaling confidence that they can manage it. This marks a potential shift in infrastructural power at the global scale – from Bretton Woods-era Western institutions towards a more multipolar arrangement. Our finding is that mBridge indeed lessens Western gatekeeping in theory, but it introduces *shared gatekeeping*: a closed club of central banks collectively deciding rules. For smaller nations, joining such a network might still mean ceding some monetary independence (since rules are set by the consortium). Yet if well-designed, it could prevent any single state from weaponizing the network unilaterally, which would be a net gain for a stable, open system.

UPI–PayNow and Regional Integration: The India–Singapore linkage of their instant payment systems offers a model of bilateral integration. UPI–PayNow went live in 2023 enabling cross-border person-to-person payments using just mobile numbers or QR codes, settling in real time at competitive forex rates (Khairnar, 2023). This has immediate benefit for migrant workers and tourists. From a gatekeeping perspective, what's interesting is that two sovereign systems learned to "speak" to each other without a global intermediary. They used cloud infrastructure and agreed standards, effectively creating a corridor-specific network. This means that to block a payment between India and Singapore now, U.S. authorities (for example) no longer have the easy option of flagging a SWIFT message – these transactions might not go through SWIFT at all. However, *new gatekeepers emerge*: in this case, the central banks of India and Singapore and their chosen tech operators. They promised the service would be low-cost and accessible to even small users (Khairnar, 2023), which is socially positive. But they also committed to compliance checks – presumably sharing data as needed to satisfy AML rules. So information could be shared between governments more directly. If, say, India wanted to monitor certain flows to Singapore (or vice versa), they likely have reciprocal access by design. So privacy might decrease even as efficiency increases (for example, using just a phone number does not mean anonymity; it's tied to your verified mobile subscriber identity). The broader implication is that regional payment integration is fragmenting the global system into interlinked hubs. The *G20 roadmap* for improving cross-border payments explicitly encourages such linkages as building blocks. This fragmentation can be good (competition, redundancy) but also complicates enforcement of global norms. A sanctioned individual might find it easier to route money through corridors outside the traditional dollar network (for example, using dirham on mBridge or rupees via UPI linkages) – unless those networks also coordinate sanctions compliance. Right now, many such projects pledge to uphold UN or FATF (Financial Action Task Force) standards, but if geopolitical blocs diverge, *compliance regimes might diverge too*. Our analysis here underscores that gatekeeping in cross-border finance is becoming a multi-polar game. Traditional hegemons (US/EU) are losing some absolute control, but it's not a free-for-all; rather, power is pooling in new configurations (consortia, bilateral pacts). This could reduce the over-reach of any one actor (preventing unilateral abuses), yet it might also reduce the efficacy of coordinated actions (like broad sanctions) against global bad actors. A concrete example: *Project mBridge has so far not been used to evade sanctions*, but Western security analysts worry it could provide an avenue for sanctioned banks to transact with each other outside the dollar system (Atlantic Council, 2025). The designers claim they can incorporate sanction screening in the platform by participants' agreement. The ultimate outcome will

depend on whether international governance frameworks can grow in tandem with these technical links – ideally to ensure these new networks are not exploited for illicit purposes, while also not becoming tools of domination by any single power.

Sanctions and AI in the New Networks: It bears noting that as payments get more data-rich and identity-tied, sanctions implementation becomes more targeted. Instead of broad country sanctions, authorities increasingly use *"surgical" sanctions at the account or transaction level*. AI tools help identify networks of shell companies or crypto addresses linked to, say, a terrorist group, and then those specific nodes can be isolated. In a CBDC scenario, if all transactions are traceable in real-time, an AI could flag and freeze assets instantaneously when blacklisted criteria are met. This is both promising for security and worrying for due process. The U.S. in 2023–24 sanctioned not just entities but specific *virtual wallet addresses*, effectively coding them as tainted. If a CBDC system had a similar feature – a global blacklist every node checks – one could *stop transactions mid-flight*. The Atlantic Council's sanctions database notes the broadening of targets to include cryptocurrency exchanges and mixers (Mortlock & Zerden, 2024). This shows regulators' intent to chase illicit flows into new platforms. We can extrapolate that future sanctions could involve instructing CBDC networks to *drop particular users or freeze certain tokens*. On the flip side, countries that oppose a sanctions policy could maintain their own networks to sustain flows. For example, Russia (facing SWIFT cut-off) accelerated work on its SPFS messaging and discussed linking to China's CIPS or CBDC to bypass SWIFT. The emergence of parallel infrastructures thus can undermine the coherence of sanction regimes, unless international agreements are refreshed. Our finding is that infrastructural power is shifting from a unipolar model to a contested networked model. While the dollar's dominance is not undone overnight, the rise of CBDCs and regional systems is *gradually chipping away* at the edges of that dominance (Atlantic Council, 2025). The next decade could see an equilibrium where multiple major currency areas each have their digital networks, interconnected by negotiated bridges. In that environment, *gatekeeping becomes a collective exercise* – for instance, a coalition can still impose sanctions, but a rival bloc might offer an alternate route. This raises the stakes for global governance: it may drive efforts for *common standards* (akin to internet governance) for digital currencies, or conversely, it may lead to a bifurcation (splinternet analogy) of monetary systems aligned with political blocs.

From a normative perspective, one can see a justice dimension here too: smaller and developing nations historically complained that the Western-led payment system and sanction regime could be unjust or overused (e.g. cutting off humanitarian trade). More diversified payment paths could provide *escape valves*, potentially reducing collective punishment effects on innocent populations. However, they could also enable malign regimes to sustain themselves financially, complicating efforts to uphold human rights. This duality underscores why an ethical analysis cannot be simplistic; it must weigh coercive power vs. restraining evil. Is it good or bad, for example, that Iran or North Korea might find it easier to transact using Chinese or Russian digital currency links? The answer might differ if we ask from the view of ordinary people vs. that of global security. Theologically, it presents a tension between judgment and mercy: sanctions are a tool of judgment (trying to force change by economic pain), but they often harm the vulnerable. Diversified systems might act as a form of *economic mercy* by preventing over-centralized strangulation of a nation, yet they might also blunt legitimate international discipline of aggressors. These are complex moral trade-offs that policymakers will increasingly face as technology outpaces the old frameworks.

4.3. Ethical and Theological Reflections: Justice, Coercion, and Conscience

A specifically Christian ontology of money views it neither as a mere instrument nor as an autonomous force, but as a covenantal social institution that symbolizes and mediates trust in economic life. Sociological accounts emphasize money's constitutive status-functions embedded in institutions (Searle, 1995; Ingham, 2004; Dodd, 2014). Critical realism clarifies that such institutions possess emergent causal powers that can enable or constrain human flourishing (Bhaskar, 2008; Archer, 1995). In the neo-Calvinist tradition, money's *structure* has a God-ordained purpose for honest exchange and stewardship, while its *direction* can be set toward idolatry or justice (Dooyeweerd, 1953/1969; Kuyper, 1898/2011; Goudzwaard, 1984; Bolt, 2013). On this view, CBDC and digital ID designs must be evaluated by whether they embody truthful weights [cf. Proverbs 11:1 (CSB)], protect the poor from domination [cf.

Proverbs 22:7 (CSB)], and leave room for mercy and periodic resets [cf. Leviticus 25 (CSB)] rather than creating architectures of totalizing control. A specifically Christian ontology of money views it neither as a mere instrument nor as an autonomous force, but as a covenantal social institution that symbolizes and mediates trust in economic life. Sociological accounts emphasize money's constitutive status-functions embedded in institutions (Searle, 1995; Ingham, 2004; Dodd, 2014). Critical realism clarifies that such institutions possess emergent causal powers that can enable or constrain human flourishing (Bhaskar, 2008; Archer, 1995). In the neo-Calvinist tradition, money's *structure* has a God-ordained purpose for honest exchange and stewardship, while its *direction* can be set toward idolatry or justice (Dooyeweerd, 1953/1969; Kuyper, 1898/2011; Goudzwaard, 1984; Bolt, 2013). On this view, CBDC and digital ID designs must be evaluated by whether they embody truthful weights [cf. Proverbs 11:1 (CSB)], protect the poor from domination [cf. Proverbs 22:7 (CSB)], and leave room for mercy and periodic resets [cf. Leviticus 25 (CSB)] rather than creating architectures of totalizing control. Grounding our discussion in theological ethics, we find both positive possibilities and grave concerns in the convergence of programmable money, digital identity, and AI governance. Scriptural principles provide a rich lens:

Economic Justice and *"Honest Scales"*: The Bible repeatedly emphasizes fairness in economic transactions – *"Dishonest scales are an abomination to the Lord, but accurate weights are His delight"* (Prov 11:1). In today's terms, this can be seen as a call for transparent and equitable financial infrastructure. If CBDCs and digital IDs are designed to *prevent fraud, ensure accurate accounting, and include the marginalized*, they resonate with the ideal of honest scales. For instance, a well-implemented CBDC could reduce exploitation by moneylenders or corrupt middlemen, by allowing the poor to receive aid directly and securely. The rich and poor would be using the same *just weights* (the same currency system with equal access), potentially narrowing systemic inequality. However, *dishonest scales* could creep in via hidden biases in algorithms or policies encoded in money. If AI transaction monitoring disproportionality flags certain groups (say, minorities or political dissidents) as "high risk" and subjects them to greater scrutiny or friction, that is an unjust weight – a form of digital bias or partiality. Likewise, if a currency is programmed to erode in value (negative interest) in a way that ordinary people cannot easily understand or avoid, one could argue this is akin to a merchant's scale subtly off-kilter – a systemic skimming. Levitical law commanded periodic resets – debts forgiven in the Sabbatical year, land returned in Jubilee (Lev 25) – to prevent permanent underclass and enshrinement of advantage. Will our digital monetary systems enable such mercy? Or will they, by their precision, eliminate the "slack" that used to allow debt jubilees? For example, in an all-digital system, a government could in theory automatically enforce all debts and taxes with precision – no debtor could escape. This might please technocrats but conflicts with the biblical notion that *creditors should not have limitless hold* over debtors (Deut 15:1-2). The Year of Jubilee (Lev 25:10) proclaimed *liberty throughout the land* – slaves freed, lands and properties returned, giving families a fresh start. If programmable finance is only used to tighten compliance (never miss a payment, or else), we risk a society with no mechanism for grace. On the other hand, one could imagine programming *automatic debt forgiveness* after a certain period, mimicking Jubilee principles – but that would require a radical policy choice, as modern economics doesn't incorporate forgiveness cycles. Our ethical stance is that justice in digital finance requires intentional features that protect the vulnerable: e.g. fee-free basic accounts, offline access for those without connectivity, privacy options so the poor are not overly surveilled, and perhaps smart contract routines that cancel micro-debts or flag when someone's subsistence would be harmed by enforcement. These would align the system more with *neighbor-love* and fairness, rather than pure efficiency or profit.

Economic Coercion and Freedom of Conscience: A core alarm raised by some theologians and laypeople relates to Revelation 13:16–17, which describes a totalitarian economic system symbolized by *the mark of the beast*: *"so that no one could buy or sell unless he had the mark"*. This apocalyptic image has made its way into public discourse whenever technological control of commerce is mentioned. While it would be hyperbolic to equate current CBDC proposals with such an ultimate evil, the concern it voices is legitimate: *Should any authority have the power to freeze an individual out of economic life entirely, especially tied to personal beliefs or allegiance?* Freedom of conscience – including religious freedom – would be gravely undermined if, for example, dissenting against a regime could result in one's money simply not working. In China, some

Christians and Muslims worry that the social credit system could, in future, penalize them economically for unauthorized gatherings or teachings. If cash disappears and only a state-linked digital currency exists, *participation in society might require implicit submission to the system's terms*, whatever they may be. This harks back to the Revelation scenario – a symbolic "mark" one must have. In less dramatic form, even Western countries could face temptations to use financial control to enforce conformity (one thinks of cases where payment platforms barred certain speech-related activities). The fusion of ID and payment makes such control technically straightforward: every transaction is attached to an identity that can be reference-checked against allowed lists. For instance, during the COVID-19 pandemic, some countries used vaccine certificates tied to QR codes for entry to venues; it's conceivable a future system might tie that to payment (can't enter store or your wallet app is disabled at entry if not compliant). These possibilities present a freedom of conscience challenge: people may feel forced to comply with mandates not just under threat of fines or jail, but under threat of being *shut out of the economy*. That is a profound power – historically akin to excommunication or ostracism, now with digital efficiency. A Christian ethical response insists that worship and allegiance cannot be coerced; economic coercion that effectively forces someone to act against their conscience (to "buy or sell") is suspect. Thus, robust legal safeguards for *due process and nondiscrimination* in digital financial networks are paramount. In democratic societies, one would argue for legislation that prohibits abuse of CBDC for political or ideological censorship. For example, a law might stipulate that *no CBDC account can be frozen without court order* and not for reasons violating civil rights (speech, religion). The *Anti-CBDC Surveillance State Act* recently passed by the U.S. House (2023) is one expression of such concerns, aiming to prevent the Federal Reserve from issuing a retail CBDC that could enable mass surveillance (US-CFS, 2024). On a global scale, there have been calls (e.g. by the IMF) for CBDC designs to include *"tiered privacy"* and ensure they do not become tools of state abuse (Atlantic Council, 2025). Our analysis affirms that freedom and human dignity must be core design principles, not afterthoughts. Otherwise, even if Revelation's beast is not literally at hand, the spirit of that warning – a world where economic life is contingent on marking loyalty to powers – could manifest in more banal, incremental ways.

Debt and Domination (Proverbs 22:7): Proverbs observes that *"the rich rule over the poor, and the borrower is slave to the lender"*. This is a realistic description of how debt creates power imbalances. In our context, one must consider whether programmable money exacerbates or mitigates debt slavery. On one hand, smart contracts could automate predatory lending – imagine a loan that auto-deducts from one's CBDC wallet every payday, with no recourse, possibly driving families into destitution if misused. On the other hand, transparency and programmability could allow regulators to enforce interest rate caps or automatic suspensions of debt repayments in hardship (like a built-in forbearance if income falls). The ethical imperative would be to structure the system such that it *serves as a tool for liberation, not oppression*. An example: In the Jubilee year, Israelite slaves were freed and land restored (Lev 25:10). Could a modern analogue be a policy where long-term credit card debt is forgiven or certain negative balances reset after X years of good behavior? Technologically, a CBDC could implement that (though economically it's complex). Conversely, if every financial action is tracked, lenders might become even more powerful (able to micro-target and pressure borrowers). We note the stark warning in Proverbs 22:7 because it reminds us that financial infrastructure is never neutral – it can entrench the dominance of the rich if unchecked. If Big Tech companies, for instance, become the primary intermediaries of CBDCs (imagine Google or Amazon managing most retail CBDC wallets), will they gatekeep access in subtle ways favoring their interests? Would they nudge people into debt-financed consumption because the data lets them? Already, fintech algorithms can profile who is a "desirable" customer. With unified digital finance, such profiling might relegate the poor to subpar services or constant monitoring. Christian ethics would demand intentional inclusion – making sure the poor are not further marginalized by digital requirements. Nigeria's initial failure to reach the unbanked with eNaira is cautionary: technology can easily leave the neediest behind or at the mercy of unscrupulous actors. A hopeful sign is some central banks discussing offline physical cards for CBDC to reach those without smartphones (for example, the Eastern Caribbean's DCash had such plans). Ensuring robust, simple access channels is a matter of justice.

Sabbath Rest in an Always-On Economy: Another theological theme is *sabbath* – the rhythm of rest and trust in God's provision. A cashless, instant,

24/7 economy intensifies the pressure to be always transacting, always optimizing. AI algorithms might even personalize prices or taxes in real time. One could ask: Will there be "rest" in such a system – moments where the churn of data stops? Theologically, a sabbath principle might inspire features like *transaction limits on Sundays* (some communities might opt for that) or at least humane policies on downtime and human override. It's speculative but worth raising that not every efficiency is humanizing. The telos (purpose) of an economy in biblical vision is to serve human flourishing in community, not to become an idol that people serve. *"No one can serve two masters… You cannot serve both God and money (mammon)"* (Matt 6:24). If the financial system becomes all-encompassing, demanding total allegiance (even if implicitly by consuming attention and governing all values), it risks becoming an object of service rather than a servant. The design of new infrastructures should keep human well-being and higher values in view – for example, providing channels for charitable giving with privacy (so donors can follow "do not let left hand know what right hand is doing"), or making sure people still have the freedom to disengage and not be penalized.

In summary of this section, our interdisciplinary evaluation finds that the programmable, data-rich payment infrastructures could either contribute to a more just and accountable economy – or facilitate an unprecedented concentration of control. The difference lies in governance choices now. Embedding *biblical ethics* such as justice, mercy, and humility into the design and policies of these systems is both a challenge and, we believe, essential. A CBDC system should ideally be judged not just by its efficiency or security, but by questions like: Does it treat the poor fairly? Does it allow room for forgiveness of mistakes? Does it uphold truth (accurate records) without destroying privacy (honoring the dignity of individuals)? Does it protect the ability to *give* and *love* (for instance, allowing anonymous alms so that giving can be pure)? These questions rarely feature in fintech design meetings, yet they could differentiate a system that truly serves humanity from one that subtly enslaves it.

5. Conclusion

This study set out to examine how the convergence of CBDCs, digital identity, ISO 20022 data standards, and AI-driven governance is reconfiguring power in payment systems, and to evaluate those changes against empirical evidence and ethical principles. Our analysis across the EU, UK, China, Nigeria, and cross-border projects yields several *key conclusions* and policy implications:

1. Infrastructural Power is Consolidating – but not Monolithic: We find that central banks and governments are, through CBDCs and digital ID linkages, consolidating greater infrastructural power *within* their jurisdictions. They are positioning themselves (or their chosen intermediaries) as the indispensable gatekeepers of all digital transactions – effectively embedding state oversight into the "DNA" of money. However, this consolidation is not uniform worldwide. In the EU and UK, it is tempered by deliberate checks (privacy options, shared governance with private sector) and a slower, consultative rollout. In China, it is accelerated and extensive, aligning with an authoritarian approach to surveillance and control. In Nigeria, the consolidation has stalled due to user resistance. ***Policy implication:*** *One-size-fits-all approaches will not work.* Each jurisdiction's approach reflects its social contract. International standard-setters (BIS, IMF) should avoid overly prescriptive models and instead promote *principles* (like interoperability, security, and privacy) that can be locally adapted. Additionally, mechanisms for *accountability* must accompany infrastructural power – e.g. independent oversight bodies for CBDC operations, transparency reports on access and usage of transaction data, and legal recourse for individuals who feel wronged by automated decisions.

2. Gatekeeping is Becoming More Fine-Grained and Programmable: The nature of financial gatekeeping is shifting from blunt instruments to fine-grained, programmable controls. Instead of "bank the unbanked" being the sole inclusion goal, we now see possibilities like "control what the banked can do with money" – a double-edged sword. The ability to set conditions on money (expiry, spend restrictions) and to instantaneously sanction or surveil means gatekeeping can happen at the micro level (transaction by transaction) (Shumba, 2023). This raises both opportunities (e.g. automatic blocking of fraud, better targeting of subsidies) and risks (e.g. micro-management of citizens' lives, chilling effects on free association if people fear being flagged). ***Policy implication:*** Governments should explicitly legislate the *permissible and impermissible uses* of programmability. For instance, one might ban

discriminatory programming (money that can only be spent by certain ethnicities or so – which sounds absurd, but technically could happen if digital ID carries demographic tags). Also, there should be *opt-out or override options* for citizens – perhaps allowing people to convert some portion of digital holdings to a bearer-instrument (like a hardware token or voucher) that isn't traced, to preserve a cash-like freedom. This could be limited for balance, but conceptually important.

3. Multi-Polar Network Governance is Needed: On the international stage, the emergence of alternative payment networks (mBridge, etc.) indicates that the unipolar era of dollar-centric payments is waning (Atlantic Council, 2025). To avoid a chaotic fragmentation (or rival blocs playing cat-and-mouse to subvert each other's sanctions and rules), there is an urgent need for *new or revitalized governance forums*. This could mean strengthening the role of the IMF or BIS in coordinating CBDC interoperability and standards on privacy, security, and legality. A framework for cross-border digital currency use – akin to treaties for the internet – should be pursued. This might cover mutual recognition of e-KYC, procedures for freeze/unfreeze requests across borders (so that criminals can't just flee to another network), and agreements on information sharing that respect sovereignty but address global crimes. Policy implication: Rather than each CBDC project operating in silo or only in like-minded clusters, the G20 and other international bodies should accelerate work on *principles for CBDCs in cross-border use*. The recent BIS Innovation Hub experiments (like Project mBridge, Project Nexus linking fast payment systems) are a start, but political backing is needed. This also ties to reforming sanctions practice: if alternative networks proliferate, major powers will need to either find new cooperative ways to enforce international norms or risk ineffectiveness. Diplomacy may thus shift toward *digital financial diplomacy* – negotiating the rules of these platforms.

4. Ethical Design is Not Optional: Our theological-ethical analysis underscores that values like equity, transparency, and human dignity should be treated as core design criteria, not afterthoughts. In practical terms, this means including diverse stakeholders (including ethicists, civil society, faith representatives) in CBDC and digital ID design discussions. It means impact assessments that specifically look at vulnerable groups. For example, *will an elderly person with no smartphone be left helpless in a CBDC-only world?* If so, mitigation like smart cards or assisted service must be planned. Or, *could an oppressive regime misuse this?* If yes, then design in limits (maybe geo-fencing certain data or requiring multi-party approval for some actions). ***Policy implication:*** Central banks and governments should publish Ethical Guidelines for Digital Currency – akin to how AI ethics frameworks are now produced. These should enshrine privacy as a right (with proportionate exceptions), commit to inclusion and accessibility, and prohibit certain exploitative features. They should also consider a *"firebreak"* for financial freedom – perhaps maintaining a parallel option (like physical cash or a decentralized e-cash token) to guarantee that people have an alternative mode of transaction that is not subject to centralized oversight, as a safeguard for civil liberties. Another implication is legal: we may need to update constitutional or human rights law to protect freedom of transaction (for lawful purposes) as a component of liberty. If tomorrow all transactions are through CBDC, something as simple as buying food is mediated by state-run systems; ensuring no one is arbitrarily denied that capability could become a rights issue.

5. Foresight – Preparing for 2035: Looking ahead ten years, we foresee a world where most major economies have introduced a CBDC (wholesale or retail), many in live operation; digital IDs are ubiquitous; ISO 20022 and successor data standards have made rich payment data the norm; and AI pervades financial decision-making. In this world, *infrastructural power will be immense*. ***The gatekeepers of 2035 might be few*** – perhaps a handful of interoperating central bank platforms and bigtech-run wallet ecosystems mediating billions of lives. To avoid negative outcomes (like oligopolies or Big Brother scenarios), actions in this decade are critical. Public engagement and literacy are essential – people should know how these systems work and have a voice in shaping them. Otherwise, apathy could lead to a situation where convenience trumps all, until a crisis reveals freedoms lost. ***The ten-year foresight*** also includes potential upheavals: maybe a major cyber attack on a CBDC network (requiring robust contingency planning, like how do we function if digital money goes down?), or a misuse scandal (e.g. a regime uses CBDC data to target a minority, leading to international backlash). Resilience – technological and social – is key. Systems should be *secure against hacking* but also *resilient against misuse by insiders*.

This may mean distributed ledger elements or multi-key authorization for critical functions.

In conclusion, the convergence of programmable CBDCs, digital IDs, ISO 20022, and AI governance indeed reconfigures who holds the "keys" to the financial system – shifting some power to central banks and governments, while also creating new nodes of influence and points of vulnerability. It holds great promise: frictionless payments, greater inclusion, better oversight of crime, and new monetary policy tools. But it also poses great peril: loss of privacy, over-centralization of authority, new forms of exclusion or manipulation. Whether infrastructural power becomes a tool of service or domination will depend on the intentional choices of design and governance we make now. As we stand at this inflection point, an *ethically grounded, interdisciplinary approach* – as we have attempted here – is vital. By heeding lessons from technology, history, and theology alike, policymakers can strive to build a monetary future that is *innovative yet just, secure yet free, unified yet humane*.

Future Research and Foresight: Several lines of inquiry demand priority as CBDCs, digital-ID wallets, ISO 20022 data rails, and AI-driven oversight mature. ***First,*** longitudinal mixed-methods studies should revisit live projects—e.g., Nigeria's eNaira, China's e-CNY, forthcoming EU/UK pilots—to track adoption, inclusion, trust, fraud, and exclusion over five- to ten-year horizons. ***Second,*** the fairness and efficacy of machine-learning models in real-time compliance screening warrant technical and ethical audits, with work on explainable AI to surface hidden biases in transaction monitoring and credit allocation. ***Third,*** governance experiments such as *mBridge* need comparative analysis of centralized, consortium, and fully distributed control structures to identify designs that curb single-actor dominance without eroding accountability. ***Fourth,*** the nascent field of economic theology should probe how digital money reshapes concepts of trust, jubilee, and hospitality, offering normative frameworks for innovations like CBDC-based UBI. ***Fifth***, applied cryptography research must test privacy-preserving proofs—e.g., zero-knowledge or anonymity vouchers—to reconcile auditability with user confidentiality. ***Sixth***, behavioral-economics work should map how perceptions of surveillance, convenience, and incentives influence spending behaviour, budgeting, and platform loyalty. ***Finally,*** scenario labs should construct integrated 2030–2035 narratives—from CBDC hegemony to stable-coin ascendance or multipolar fragmentation—to stress-test monetary policy tools, cyber-resilience, and civil-liberties safeguards.

Limitations: This study synthesizes the best available secondary data, yet its conclusions face six constraints. First, most CBDCs remain in pilot or early launch; adoption, sanction-evasion efficacy, and social impacts are therefore provisional and may shift with fuller roll-outs or policy pivots. Second, the geographic sample—EU, UK, China, Nigeria, and two cross-border corridors—excludes regions such as Latin America or Scandinavia, limiting generalizability across diverse regulatory cultures. Third, integrating technical, political, and theological literatures risks interpretive gaps or overextension of scriptural analogies, despite careful source triangulation. Fourth, our normative inclination toward privacy and decentralization may colour risk assessments, even as we report official goals and efficiencies. Fifth, we touch only lightly on adjacent technologies—quantum-safe cryptography, IoT micropayments, DeFi–CBDC hybrids—that could alter future gatekeeping dynamics. Sixth, the absence of primary stakeholder interviews means lived experiences of unbanked users, fintech builders, and regulators are inferred rather than directly voiced. These constraints counsel caution: findings should be read as an analytically grounded baseline, open to refinement through longitudinal data, broader case coverage, deeper tech forensics, and participatory field research.

Conflict of Interest: The authors have no conflicts of interest to disclose.

Funding: This manuscript was prepared entirely through the authors' own efforts and resources; no external funding was received.

Author Contributions (CRediT taxonomy): **Conceptualization:** S. Sangwa. **Methodology:** S. Sangwa. **Investigation:** S. Sangwa and P. Mutabazi. **Data curation:** S. Sangwa. **Formal analysis:** S. Sangwa. **Visualization:** S. Sangwa. **Writing – original draft:** S. Sangwa. **Writing – review and editing:** S. Sangwa and P. Mutabazi. **Supervision:** P. Mutabazi. **Project administration:** S. Sangwa. All authors meet Taylor & Francis authorship criteria and have reviewed and approved the final version of the manuscript.

Artificial-Intelligence Assistance: The authors employed the generative large-language model ChatGPT (OpenAI GPT-4o, accessed 01 August 2025) for two limited purposes: first, to refine grammar, wording, and stylistic clarity, and second, to expedite the identification of publicly available scholarly sources relevant to the manuscript's themes. A representative prompt was, "Please help me improve the following paragraph to ensure correct English grammar and suggest peer-reviewed studies published since 2020 on this topic." The model did not generate original ideas, data, analyses, or visualizations. All AI-suggested edits and literature leads were manually verified for accuracy, intellectual rigor, and proper attribution. The authors accept full responsibility for the final content.

References

AP News/ABC News wire. (2024, July). China is expanding into digital currencies, hoping to promote use of its 'people's money'. https://apnews.com/article/stablecoin-currency-china-yuan-dollar-trump-fdc6bf0df8629e542f18fab50f5d32fd

Archer, M. S. (1995). *Realist social theory: The morphogenetic approach*. Cambridge University Press. https://doi.org/10.1017/CBO9780511557675

Associated Press. (2024, Oct 12). China is expanding into digital currencies, hoping to promote use of its 'people's money'. https://apnews.com/article/stablecoin-currency-china-yuan-dollar-trump-fdc6bf0df8629e542f18fab50f5d32fd

Auer, R., Frost, J., Gambacorta, L., Monnet, C., Rice, T., & Shin, H. S. (2022). Central bank digital currencies: Motives, economic implications, and the research frontier. *Annual Review of Economics, 14*, 697–721. https://doi.org/10.1146/annurev-economics-051420-020324

Aune, D. E. (1998). *Revelation 6–16* (Vol. 52B). Word. https://dokumen.pub/revelation-6-16-volume-52b-word-biblical-commentary-9780310521709-031052170x.html

Atlantic Council. (2025, July). *Central Bank Digital Currency (CBDC) Tracker*. https://www.atlanticcouncil.org/cbdctracker/

Bank for International Settlements (BIS). (2024, November 11). *Project mBridge reached the minimum viable product stage*. https://www.bis.org/about/bisih/topics/cbdc/mcbdc_bridge.htm

Bank for International Settlements. (2024). *Advancing in tandem: Results of the 2024 BIS survey on CBDCs and crypto* (BIS Papers No. 159). https://www.bis.org/publ/bppdf/bispap159.pdf

Bank of England. (2023). *ISO 20022 handbook* (CHAPS migrated 19 June 2023). https://www.bankofengland.co.uk/payment-and-settlement/rtgs-renewal-programme/iso-20022-handbook

Bank of England & HM Treasury. (2023). *The digital pound: A new form of money for households and businesses?* Consultation Paper.https://www.bankofengland.co.uk/paper/2023/the-digital-pound-consultation-paper

Beale, G. K. (1999). *The Book of Revelation: A commentary on the Greek text* (NIGTC). Eerdmans. https://dokumen.pub/the-book-of-revelation-a-commentary-on-the-greek-text-080282174x-0833648514.html

Bhaskar, R. (2008). *A realist theory of science* (4th ed.). Routledge. https://doi.org/10.4324/9780203090732

Central Bank of The Bahamas. (2024, September 26). *Sand Dollar in circulation and usage update*. https://www.centralbankbahamas.com/news/press-releases/press-release-public-update-on-the-bahamas-digital-currency-sanddollar-3

Committee on Payments and Market Infrastructures (CPMI). (2023, October). *Harmonised ISO 20022 data requirements for enhancing cross-border payments* (Report No. CPMI d218). Bank for International Settlements. https://www.bis.org/cpmi/publ/d218.pdf

Dodd, N. (2014). *The social life of money*. Princeton University Press. https://doi.org/10.1017/beq.2016.39

Dooyeweerd, H. (1969). *A new critique of theoretical thought* (Vols. 1–4). Presbyterian & Reformed. (Orig. work published 1953–1958). https://archive.org/details/nctt-vol1

European Central Bank (ECB). (2023, October 17). *ECB welcomes the CPMI's report on harmonised ISO 20022 data requirements for cross-border payments*. https://www.ecb.europa.eu/press/intro/news/html/ecb.mipnews231017.en.html

European Central Bank. (2023, March 21). Successful launch of new T2 wholesale payment system [Press release].

https://www.ecb.europa.eu/press/pr/date/2023/html/ecb.pr230321~f5c7bddf6d.en.html

European Central Bank. (2024, June 24). *ECB publishes first progress report on digital euro preparation phase* [Press release].https://www.ecb.europa.eu/press/pr/date/2024/html/ecb.pr240624~7b3d7581e6.en.html

European Commission & Parliament. (2024). *Regulation (EU) 2024/1183 on a framework for a European digital identity*. https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng

European Union (EU). (2024). *The establishment of the European Digital Identity Framework, including the provision of European Digital Identity Wallets and trust services*. EUR-Lex. Retrieved from https://eur-lex.europa.eu/EN/legal-content/summary/the-establishment-of-the-european-digital-identity-framework-including-the-provision-of-european-digital-identity-wallets-and-trust-services.html

Farrell, H., & Newman, A. L. (2019). Weaponized interdependence. *International Security, 44*(1), 42–79. https://doi.org/10.1162/isec_a_00351

Foucault, M. (2007). *Security, territory, population: Lectures at the Collège de France, 1977–1978* (G. Burchell, Trans.). Palgrave Macmillan. https://www.bis.org/publ/bppdf/bispap159.pdf

Goudzwaard, B. (1984). *Idols of our time*. InterVarsity Press. https://archive.org/details/idolsofourtime0000goud_o0m8

Hume, E., & Rutter, K. (2025, March 11). *Sanctions by the Numbers: 2024 Year in Review* [Report]. Center for a New American Security. https://www.cnas.org/publications/reports/sanctions-by-the-numbers-2024-year-in-review

Ingham, G. (2004). *The nature of money*. Polity. https://dl.fqhci.com/library/Crypto/economy-money/En/the-nature-of-money-geoffrey-ingham.pdf

International Monetary Fund. (2024, May 6). *Nigeria: 2024 Article IV Consultation—Press release; staff report; and statement by the Executive Director for Nigeria*. https://www.imf.org/en/Publications/CR/Issues/2024/05/08/Nigeria-2024-Article-IV-Consultation-Press-Release-Staff-Report-Staff-Statement-and-548726

Khairnar, S. (2023, February 21). *Singapore and India link up PayNow and UPI for real-time cross-border payments*. FinTech Futures. https://www.fintechfutures.com/cross-border-payments/singapore-and-india-link-up-paynow-and-upi-for-real-time-cross-border-payments

Koester, C. R. (2014). *Revelation* (AYB 38A). Yale University Press. https://yalebooks.yale.edu/book/9780300216912/revelation/

Kuyper, A. (2011). *Lectures on Calvinism*. Hendrickson. (Orig. lectures 1898–1899). https://archive.org/details/calvinismsixst00kuyp

Krippendorff, K. (2018). *Content analysis: An introduction to its methodology* (4th ed.). Sage. https://doi.org/10.4135/9781071878781

Illes, A., Kosse, A., & Wierts, P. (2025). *Advancing in tandem - results of the 2024 BIS survey on central bank digital currencies and crypto*. BIS Papers No. 159. Retrieved from https://www.bis.org/publ/bppdf/bispap159.pdf

Ledger Insights. (2023, May 22). *IMF report explores Nigeria's slow CBDC adoption, future remittance use*. https://www.ledgerinsights.com/imf-nigeria-slow-cbdc-adoption/

Mann, M. (1984). The autonomous power of the state: Its origins, mechanisms and results. *European Journal of Sociology, 25*(2), 185–213. https://doi.org/10.1007/s10677-009-9212-4

Mortlock, D., & Zerden, A. (2024, January). *Sanctions have become a tool of first resort, but enforcement needs upgraded and updated resources* (Issue Brief). Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/sanctions-have-become-a-tool-of-first-resort/

Payments Canada. (2023, March 21). *Payments Canada introduces data-rich messages to high-value payments in Canada with Lynx Release Two*. https://www.payments.ca/payments-canada-introduces-data-rich-messages-high-value-payments-canada-lynx-release-two

People's Bank of China. (2021). *Progress of research & development of e-CNY in China* (White paper). https://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021072014364791207.pdf

People's Bank of China figures via China Daily. (2022, October 12). Digital yuan trading value

tops 100 billion yuan. https://www.chinadaily.com.cn/

Reuters. (2024, May 17). Hong Kong allows China's digital yuan to be used in local shops. https://www.reuters.com/markets/currencies/hong-kong-allows-chinas-digital-yuan-be-used-local-shops-2024-05-17/

Rose, N. (1999). *Powers of freedom: Reframing political thought*. Cambridge University Press. https://doi.org/10.1017/CBO9780511488856

Sayer, A. (2000). *Realism and social science*. Sage. https://us.sagepub.com/en-us/nam/realism-and-social-science/book207971

Searle, J. R. (1995). *The construction of social reality*. Free Press. Available from: https://philpapers.org/rec/SEATCO

Shenzhen Municipal (via *China Daily*). (2023, July 18). Shenzhen sets up over 35m e-CNY wallets; >2.1m merchants accept e-CNY. https://global.chinadaily.com.cn/a/202307/18/WS64b6398fa31035260b817102.html

Shumba, C. (2023, June 16). *Central Banks successfully test over 30 CBDC use cases, including offline payments*. CoinDesk. https://www.coindesk.com/policy/2023/06/16/central-banks-successfully-test-more-than-30-cbdc-use-cases-including-offline-payments

Soana, G., de Arruda, T. (2024). Central Bank Digital Currencies and financial integrity: finding a new trade-off between privacy and traceability within a changing financial architecture. *J Bank Regul* 25, 467–486. https://doi.org/10.1057/s41261-024-00241-2

Taylor, C. (2004). *Modern social imaginaries*. Duke University Press. https://www.dukeupress.edu/modern-social-imaginaries

Unlock Blockchain. (2025, September 5). CBDCs between progress and stagnation: BIS 2024 survey in perspective. Unlock Blockchain. https://www.unlock-bc.com/148310/bis-2024-cbdc-survey/

United States Federal Reserve Financial Services. (2025, February 13). *ISO® 20022 implementation rescheduled to July 14 for the Fedwire® Funds Service*. https://www.frbservices.org/news/communications/021325-fedwire-iso20022-implementation-rescheduled-July-14

United States Federal Reserve Financial Services. (2025, June 17). *One month to go for Fedwire Funds Service ISO 20022 implementation*. https://www.frbservices.org/news/fed360/issues/061725/wires-one-month-to-go-contingency

University Consortium (UC). (2021, February 11). *Henry Farrell and Abraham Newman: Weaponized interdependence* (Recording and summary of a talk delivered at a UC online pre-Module event). University Consortium, University of Oxford. https://uc.web.ox.ac.uk/article/henry-farrel-and-abraham-newman-weaponized-interdependence

U.S. House Committee on Financial Services (US-CFS). (2024, May 23). *House passes CBDC Anti-Surveillance State Act*. https://financialservices.house.gov/news/documentsingle.aspx?DocumentID=409278

Victoria Cleland, Bank of England. (2023, October). ISO 20022: Reaping the benefits for the payments ecosystem. https://www.bankofengland.co.uk/-/media/boe/files/speech/2023/october/iso-20022-reaping-the-benefits-for-the-payments-ecosystem-victoria-cleland-slides.pdf

Zelizer, V. A. (1994). *The social meaning of money*. Basic Books. https://press.princeton.edu/books/paperback/9780691176031/the-social-meaning-of-money?srsltid=AfmBOoo8adWc2ur5ZVl4Zo6do-kioqcpQfK3y-OoGMwO5LL7pkVeVRB